**Trust, Security, and Resilience for 6G Systems**

# Executive Summary

The introduction of 5G networks has seen the manifestation of a desire to accommodate use cases of a more critical nature that span broad societal objectives, including critical use cases that seek to automate manufacturing, process control, utilities, transportation, logistics etc. It has become apparent that the level of performance, security, and resilience demanded by many of these scenarios will significantly alter the landscape of attack surfaces presented by faults, disturbances, threats, and anomalies within the connectivity and computational services provided by the network. Additionally, it has become clear that there is an imminent need to eliminate all single points of failure and to architect a network based on zero-trust principles in a manner that affords users high levels of reliability along with attention to availability and functional safety, and privacy. The development of 6G technologies will accommodate these needs more effectively, even as we continue to improve standalone 5G systems to meet immediate concerns associated with earlier design choices.

Trustworthiness is defined in this paper as confidence in the ability of the 6G system to perform as expected in the face of environmental disturbances, impairments, errors, faults, and attacks. This definition of trustworthiness has several proof points specific to the establishment of information and Communications Technologies (ICT) and pertinent to 6G:

1. Business processes and economic value chains are organized not to create doubt or a lack of confidence in equipment, actors, and processes associated with network services.

2. Diligence in developing standards that can be tested and certified for consistency with well-defined requirements.

3. Networks and associated services that are secure, privacy preserving, reliable, available, and resilient.

4. Assurance that the network equipment and associated services are interoperable across the ecosystem and that networks are deployed and operated in accordance with the expectations of users.

As we evolve the network to 6G, we will be adding new applications that enhance digital world experiences utilizing the Internet of senses and improvements related to extended reality (XR) capabilities. While cellular technologies can be deployed to serve all these use cases, it has been challenging to establish the ability of these technologies to meet the security, privacy, and resilience requirements demanded by those industry stakeholders. Stakeholders have concern about the adoption of wireless technologies into their workflows: cyber-attacks, privacy violations, data theft, exposure of vulnerabilities due to the introduction of distributed cloud computation and storage, and the increased use of AI through adaptive learning algorithms that will depend on assurance of data integrity, privacy, and explainability. Governments have concerns about the trustworthiness of the supply chain and the ecosystem's ability to overcome dynamic threats rapidly.

**Key Points:**

This paper offers five research directions that will greatly aid the objective of trust, security and resilience for 6G systems:

1. Security Assurance and Defense: use of techniques like Common Criteria (CC) as a part of a comprehensive security assurance process, zero-trust architectures, trustworthy and explainable AI/ML architectures, use of AI for security defense etc.
2. Confidential Computing: protection of confidential and proprietary data, secrecy for cryptographic computation, hardware-based confidential computation, homomorphic encryption, multi-party computation etc.
3. Secure Identities and Protocols: privacy enhancing technologies, anonymous and ephemeral credentials, elimination of information leakage, transparency towards service availability, attestation of functions, hardware, and interfaces.
4. Service Availability: Assurance for service availability, response mechanism to security threats, reconfigurability and mobility of computational resources, end-to-end observability, redundancy, multi-path transport etc.
5. Post-Quantum Cryptography: protection of cryptographic algorithms against quantum computation, hardening of cryptographic protocols, quantum encryption, quantum key distribution.

The paths to realizing the technological solutions for trust and resilience will reside with various actors and stakeholders. Standards organizations such as the 3GPP and the IETF will play an important role in developing access-specific functionality and integrating Internet technologies. Governmental organizations such as NIST are important participants in the standards process and are a valuable resource in North America. Lastly, we expect a partnership between the NSF, industry, and academic institutions towards realizing a high degree of security, privacy, safety, and resilience from 6G networks.

**Callouts:**

* Executive summary
	+ Trustworthiness is defined as confidence in the ability of the 6G system to perform as expected in the face of environmental disturbances, impairments, errors, faults, and attacks.
* Section 1, last paragraph:
	+ People, businesses, and governments will trust the 6G system to be resilient, secure, privacy-preserving, safe, reliable, dependable, and available under all circumstances.
* Section 2,

The operational aspects of the trustworthy 6G network will be based on an automated approach to security assurance and defense, and a strong focus on performance management.

* Section 3.1:
* Section 3.2:
* Section 3.3:
	+ In 6G, confidential compute technologies and Root-of-Trust attestation can be used to secure the orchestration and storage of identities in a verifiable and trustworthy manner.
* Section 3.5:
	+ 6G networks should be ready to use advances in quantum computing. Network coding with post-quantum security must be used to provide end-to-end confidentiality.
* Section 4:
	+ Industry action must consider the interaction between 6G and 5G towards reducing the vulnerabilities of 6G due to backward compatibility requirements.